



# Certification Report

## NetScout nGenius® 3900 Series Packet Flow Switch

Issued by:

**Communications Security Establishment**

**Certification Body**

**Canadian Common Criteria Evaluation and Certification Scheme**

© Government of Canada, Communications Security Establishment, 2015

**Document number:** 383-4-281-CR  
**Version:** 1.0  
**Date:** 25 November 2015  
**Pagination:** i to iii, 1 to 8



**DISCLAIMER**

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

## FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provide a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CSC Security Testing/Certification Laboratories.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 25 November 2015, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarks or registered trademarks:

- NetScout and nGenius are registered trademarks of NetScout Systems, Inc.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

**TABLE OF CONTENTS**

**Disclaimer ..... i**

**Foreword..... ii**

**Executive Summary ..... 1**

**1 Identification of Target of Evaluation..... 2**

**2 TOE Description ..... 2**

**3 Security Policy ..... 3**

**4 Security Target..... 3**

**5 Common Criteria Conformance..... 3**

**6 Assumptions and Clarification of Scope..... 4**

    6.1 SECURE USAGE ASSUMPTIONS..... 4

    6.2 ENVIRONMENTAL ASSUMPTIONS ..... 4

**7 Evaluated Configuration ..... 4**

**8 Documentation ..... 5**

**9 Evaluation Analysis Activities ..... 5**

**10 ITS Product Testing..... 6**

    10.1 INDEPENDENT FUNCTIONAL TESTING ..... 6

    10.2 INDEPENDENT PENETRATION TESTING..... 6

    10.3 CONDUCT OF TESTING ..... 6

    10.4 TESTING RESULTS..... 6

**11 Results of the Evaluation..... 6**

**12 Evaluator Comments, Observations and Recommendations ..... 7**

**13 Acronyms, Abbreviations and Initializations..... 7**

**14 References ..... 8**

## Executive Summary

NetScout nGenius® 3900 Series Packet Flow Switch (hereafter referred to as nGenius® 3900 Series PFS), from NetScout Systems, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that nGenius® 3900 Series PFS is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

The nGenius® 3900 Series PFS provides selective packet-flow access to an increasing number of task-specific management tools. nGenius® 3900 Series PFS is an extensible chassis-based, data center class network monitoring switch that enables access to network traffic across distributed networks for use by any network monitoring, performance management and security system.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 25 November 2015 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for nGenius® 3900 Series PFS, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the CCS Certification Body, declares that the nGenius® 3900 Series PFS evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

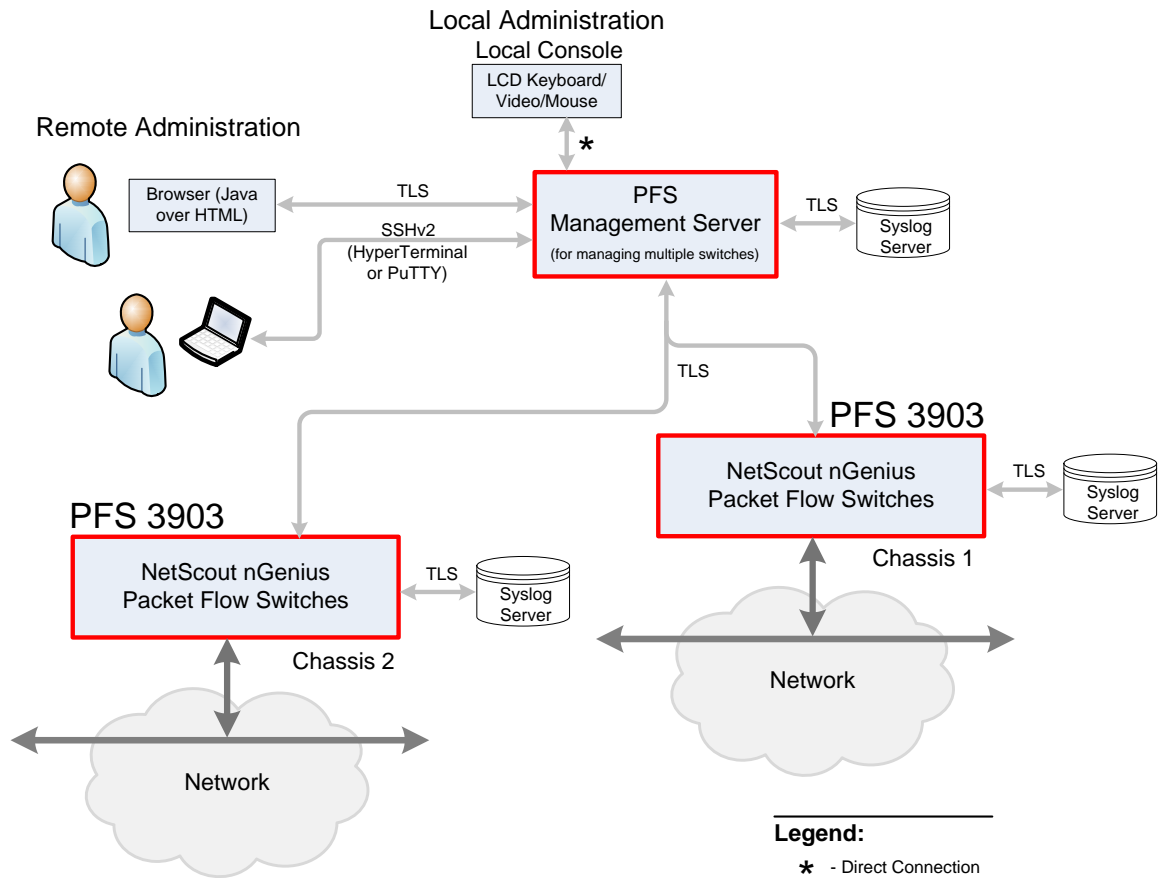
## 1 Identification of Target of Evaluation

NetScout nGenius® 3900 Series Packet Flow Switch (hereafter referred to as nGenius® 3900 Series PFS), from NetScout Systems, Inc., is the Target of Evaluation. The nGenius® 3900 Series PFS is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

## 2 TOE Description

The nGenius® 3900 Series PFS provides selective packet-flow access to an increasing number of task-specific management tools. nGenius® 3900 Series PFS is an extensible chassis-based, data center class network monitoring switch that enables access to network traffic across distributed networks for use by any network monitoring, performance management and security system.

A diagram of the nGenius® 3900 Series PFS architecture is as follows;



### 3 Security Policy

nGenius® 3900 Series PFS implements a role-based access control policy to control administrative access to the system. In addition, nGenius® 3900 Series PFS implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access
- Trusted Path/Channels

The following cryptographic module was evaluated to the FIPS 140-2 standard:

Cryptographic Module	Certificate #
OpenSSL FIPS Object Module	1747

### 4 Security Target

The ST associated with this Certification Report is identified below:

NetScout Systems Inc. nGenius® 3900 Series Packet Flow Switch with software version 3.3.40, Security Target, version 1.0, 24 November 2015.

### 5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*.

nGenius® 3900 Series PFS is:

- a. Conformant to the Protection Profile for Network Devices, v1.1, June 8, 2012,
- b. *Common Criteria Part 2 extended*, with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
  - FAU\_STG\_EXT.1 - External audit trail storage
  - FCS\_CKM\_EXT.4 - Cryptographic key zeroization
  - FCS\_RBG\_EXT.1 - Cryptographic operation: random bit generation
  - FCS\_HTTPS\_EXT.1 - HTTPS
  - FCS\_TLS\_EXT.1 - TLS
  - FIA\_PMG\_EXT.1 - Password management
  - FIA\_UIA\_EXT.1 - User identification and authentication
  - FIA\_UAU\_EXT.2 - Password-based authentication mechanism

- FPT\_SKP\_EXT.1 - Protection of TSF data
  - FPT\_APW\_EXT.1 - Protection of administrator passwords
  - FPT\_TUD\_EXT.1 - Trusted update
  - FPT\_TST\_EXT.1 - TSF testing
  - FTA\_SSL\_EXT.1 - TSF-initiated session locking
- c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

## 6 Assumptions and Clarification of Scope

Consumers of nGenius® 3900 Series PFS should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

### 6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE; and
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

### 6.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

## 7 Evaluated Configuration

The evaluated configuration for nGenius® 3900 Series PFS comprises:

One or more instances of the nGenius® 3900 Series PFS which is made up of either the PFS 3901 single slot chassis or PFS 3903 three slot chassis in single or multiple chassis.

For administering multiple chassis, a standalone dedicated PFS Management Server must be used for user administration and device configuration. A single chassis can be managed by the embedded management server or by the PFS Management Server. The PFS Management Server is able to manage both the single or multiple chassis.

*The publication entitled Common Criteria Supplemental Guidance for nGenius PFS Management Server and PFS Switch Software Version 3.3.4 (Part Number 733-0504 Rev. A) describes the procedures necessary to install and operate nGenius® 3900 Series PFS in its evaluated configuration.*



## 8 Documentation

The NetScout Systems, Inc. documents provided to the consumer are as follows:

- *nGenius® 3900 Series Packet Flow Switch Hardware Installation Guide* (Part Number 733-0596 Rev. A);
- *nGenius® 3901R Packet Flow Switch Quick Connection Guide* (Part Number 293-2567 Rev. A);
- *nGenius® 3903 Packet Flow Switch Quick Connection Guide* (Part Number 293-2568 Rev. A);
- *nGenius® PFS Management Software Administrator Guide* (Part Number 733-0595 Rev. B);
- *nGenius® PFS Management Server Hardware Installation Guide* (Part Number 293-2566 Rev. A);
- *nGenius® 3900 Series Packet Flow Switch v3.3 Release Notes* (Part Number 733-0672 Rev. A); and
- *Common Criteria Supplemental Guidance for nGenius PFS Management Server and PFS Switch Software Version 3.3.4* (Part Number 733-0504 Rev. A).

## 9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of nGenius® 3900 Series PFS, including the following areas:

**Development:** The evaluators analyzed the nGenius® 3900 Series PFS functional specification and determined that the functional specification describes the purpose and method of use for each TSF interface and that the nGenius® 3900 Series PFS functional specification is an accurate and complete instantiation of the SFRs.

**Guidance Documents:** The evaluators examined the nGenius® 3900 Series PFS preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

**Life-cycle support:** An analysis of the nGenius® 3900 Series PFS configuration management system and associated documentation was performed. The evaluators found that the nGenius® 3900 Series PFS configuration items were clearly marked.

All these evaluation activities resulted in **PASS** verdicts.

## 10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

### 10.1 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

- a. NDPP required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the NDPP to which the TOE is claiming conformance.

### 10.2 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- a. NDPP required assurance activities. The evaluator performed the assurance activities mandated by the protection profile to which the TOE is claiming conformance; and
- b. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

### 10.3 Conduct of Testing

nGenius® 3900 Series PFS was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test Facility. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

### 10.4 Testing Results

The independent tests yielded the expected results, providing assurance that nGenius® 3900 Series PFS behaves as specified in its ST and functional specification.

## 11 Results of the Evaluation

This evaluation has provided the basis for a NDPP conformance claim as claimed in Section 5. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

## 12 Evaluator Comments, Observations and Recommendations

The evaluator recommends that users follow the Common Criteria Supplemental Guidance for nGenius PFS Management Server and PFS Switch Software Version 3.3.4 (Part Number 733-0504 Rev. A) closely, if they wish to deploy the evaluated configuration. Users should contact NetScout Support if they have any questions or concerns about the advice provided within the Common Criteria Supplemental Guidance. Departure from the evaluated configuration should only be performed in consideration of the deployment scenario and associated risk profile.

## 13 Acronyms, Abbreviations and Initializations

<u>Acronym/Abbreviation/Initialization</u>	<u>Description</u>
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PFS	Packet Flow Switch
PALCAN	Program for the Accreditation of Laboratories - Canada
NDPP	Protection Profile for Network Devices
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

## 14 References

This section lists all documentation used as source material for this report:

- a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.
- b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
- c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
- d. Protection Profile for Network Devices, v1.1, June 8, 2012.
- e. NetScout Systems Inc. nGenius® 3900 Series Packet Flow Switch with software version 3.3.40, Security Target, version 1.0, 24 November 2015.
- f. Evaluation Technical Report NetScout nGenius® 3900 Series Packet Flow Switch with P-Blade and software version 3.3.40 build #32 and NetScout nGenius® PFS Management Server with software version 3.3.40 build #32, version 1.0, 25 November 2015.